Based on the initial post and the feedback from peers, further proof that Zero Trust Network (ZTN) and Microservice Architecture (MA) are the trends for service delivery in the organization. Broadly speaking, the operation and implementation could be challenging. Organizations must consider the balance on the security level and convenience of their users.

As regards on Zero Trust Network, Jonathan (2021) mentioned that the use of Multi-factor Authentication (MFA) to be in the balance. It could reduce the number of authentications for a period to for the low-risk activity like log in or check balance, on the other hand, have the MFA each time for the high-risk activity like payment transaction or changing password. It could mitigate the concern of task efficiency which Jonathan (2021) highlighted. With reference to the adopt reason of MFA in Yubico and 451 research (Zander, 2021) found that the main obstacles are user experience, complexity, and cost for the organization adoption. Despite that current authentication methods such as biometrics and modern MFA have been shown to be more secure and usable than legacy MFA systems. Austin (2021) stated that the cyber-attacks will evolve to target businesses that without implemented zero trust, demonstrated how critical it is for organizations to implement a ZTN.

Meanwhile, for the Microservice Architecture, Kingsley (2021) further explained that the authentication extends to authenticating individual packets. It could use the encrypted Application Programming Interface (API) to secure the network traffic. It is partially right about MA discourages reusing code by Kingsley (2021). Sharing code for different microservices would cause the falling of dependencies, beating the ultimate purpose of MA. Except for microservice itself, there are challenges on code reusability between different microservices which could not be simply replicate. To improving the reusability, the MA team could identify several reusable codes as common components or packages which have similar logic that can be used across microservices (Ashan, 2019).

To sum up, ZTN and MA have become a common practice for internet service delivery, especially in the bank system. Encryption like token authentication and SSL are build-in functions and even enabled by default on the software designed, which encouraging the peripheral system to compliant with. This should not be a matter of whether to use or not to use, but of how to use instead.

References:

Zander, W. (April 26, 2021) Multi-factor authentication adoption: 75% of enterprise security managers plan to increase MFA spending according to new study by Yubico and 451 Research. *2021 Yubico and 451 Research Study.* Available from: https://www.yubico.com/blog/75-of-enterprise-security-managers-plan-to-increase-mfa-spending-according-to-new-study-by-yubico-and-451-research/ [Accessed 1 October 2021].

Ashan, F. (Nov 13, 2019) The Dilemma of Code Reuse in Microservices. *Bits and Pieces*. Available from: https://blog.bitsrc.io/the-dilemma-of-code-reuse-in-microservices-a925ff2b9981 [Accessed 1 October 2021].